

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 63-298588

(43)Date of publication of application : 06.12.1988

(51)Int.Cl.

G06K 19/00

B42D 15/02

G06K 17/00

(21)Application number : 62-131269

(71)Applicant : HITACHI MAXELL LTD

(22)Date of filing : 29.05.1987

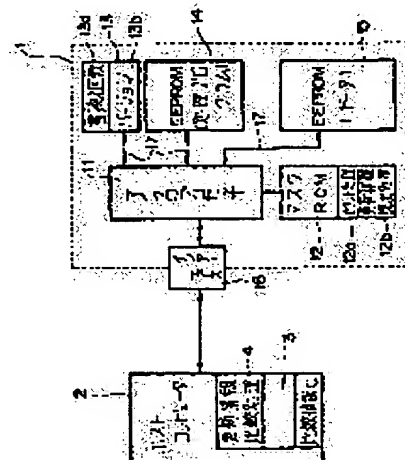
(72)Inventor : YAMAUCHI AKIRA
SUGAWARA TAKESHI
SHINAGAWA TORU

(54) IC CARD AND ITS INFORMATION PROCESSING SYSTEM

(57)Abstract:

PURPOSE: To check an IC card which has been rewritten fraudulently, by storing in advance updating information in an storage mean electrically erasable at the IC card side, reading out the updating information at a host computer side to which the IC card is inserted, and comparing it with updating information at the host computer side.

CONSTITUTION: Updating information which is updated automatically in accordance with rewriting of a processing program, etc. is stored in advance in an electrically erasable storage means (EEPROM 13) of an IC card 1 side, and also, this updating information can be read out as necessary. In this state, the updating information is read out at a host computer 2 side to which the IC card 1 is inserted, and compared with updating information at the host computer 2 side. Accordingly, whether the processing program has been rewritten by others than the host computer 2 or not can be detected. In such a way, the IC card 1 which has been rewritten fraudulently can be checked.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the
examiner's decision of rejection or application converted
registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of
rejection][Date of requesting appeal against examiner's decision of
rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A)

昭63-298588

⑬ Int. Cl.⁴ 識別記号 庁内整理番号 ⑭ 公開 昭和63年(1988)12月6日
G 06 K 19/00 N-6711-5B
B 42 D 15/02 J-8302-2C
G 06 K 17/00 D-6711-5B 審査請求 未請求 発明の数 2 (全7頁)

⑮ 発明の名称 ICカード及びその情報処理システム

⑯ 特 願 昭62-131269

⑰ 出 願 昭62(1987)5月29日

⑱ 発 明 者 山 内 暁 大阪府茨木市丑寅1丁目1番88号 日立マクセル株式会社
⑲ 発 明 者 菅 原 健 大阪府茨木市丑寅1丁目1番88号 日立マクセル株式会社
⑳ 発 明 者 品 川 徹 大阪府茨木市丑寅1丁目1番88号 日立マクセル株式会社
㉑ 出 願 人 日立マクセル株式会社 大阪府茨木市丑寅1丁目1番88号
㉒ 代 理 人 弁理士 梶山 信是 外1名

明 細 書

1. 発明の名称

ICカード及びその情報処理システム

2. 特許請求の範囲

- (1) 演算処理装置とこの演算処理装置が実行する第1の処理プログラム、そのデータ及び更新情報を記憶する消去可能な第1の記憶手段と前記演算処理装置が実行する消去不可能な第2の処理プログラムを記憶する第2の記憶手段とを備え、前記第1の処理プログラムは挿着される情報処理装置側から書込まれるものであり、前記更新情報は第1の処理プログラムの全部又は一部が書換えられたときに書換えられた回数を示し、第2の処理プログラムは前記情報処理装置からの制御信号に応じて第1の処理プログラムの全部若しくは一部の書込み、前記更新情報の読出し及び第1の処理プログラムの全部若しくは一部の書込みに応じて前記更新情報の値を加算若しくは減算する処理を行うことを特徴とするICカード。
- (2) 更新情報は第1の処理プログラムの全部又は

一部が読出されたときに読出された回数を示すものであり、第2の処理プログラムは情報処理装置からの制御信号に応じて第1の処理プログラムの全部若しくは一部の読出し、前記更新情報の読出し及び第1の処理プログラムの全部若しくは一部の読出しに応じて前記更新情報の値を加算若しくは減算する処理を行うことを特徴とする特許請求の範囲第1項記載のICカード。

(3) 演算処理装置とこの演算処理装置が実行する第1の処理プログラム、そのデータ及び更新情報を記憶する消去可能な第1の記憶手段と前記演算処理装置が実行する消去不可能な第2の処理プログラムを記憶する第2の記憶手段とを有するICカードと、このICカードが挿着されたときこのICカードとデータの授受を行いかつ前記第1の処理プログラムを有して前記ICカードにこれを書込む制御をする情報処理装置とを備え、前記更新情報は第1の処理プログラムの全部又は一部が書換えられたときに書換えられた回数を示し、第2の処理プログラムは前記情報処理装置からの

制御信号に応じて第1の処理プログラムの全部若しくは一部の書込み、前記更新情報の読出し及び第1の処理プログラムの全部若しくは一部の書込みに応じて前記更新情報の値を加算若しくは減算する処理を行うものであることを特徴とするICカード情報処理システム。

(4) 情報処理装置は第1の処理プログラムと更新情報とを有してICカードに第1の処理プログラムを書込む制御をし、第1の処理プログラムの全部若しくは一部を前記ICカードに書込むとき又は書込んだときに自己の更新情報を更新し、前記ICカードが挿着されたときに挿着されたICカードから更新情報を読出して自己の更新情報と相違するか否かを判定して一致していないときには前記挿着されたICカードとのデータの授受を行わないことを特徴とする特許請求の範囲第3項記載のICカード情報処理システム。

(5) 更新情報は更新回数を示す第1の更新情報と第1の処理プログラムの更新に応じて情報処理装置から書込まれる第2の更新情報とからなり、前

記情報処理装置は第1の処理プログラムと第1及び第2の更新情報とを有してICカードに第1の処理プログラムと第2の更新情報とを書込む制御をし、第1の処理プログラムの全部若しくは一部を前記ICカードに書込むとき又は書込んだときに自己の第1の更新情報を更新し、前記ICカードが挿着されたときに挿着されたICカードから第1の更新情報及び第2の更新情報を読出して自己の第1の更新情報及び第2の更新情報と相違するか否かを判定して一致していないときには前記挿着されたICカードとのデータの授受を行わないことを特徴とする特許請求の範囲第3項記載のICカード情報処理システム。

3. 発明の詳細な説明

〔産業上の利用分野〕

この発明は、ICカード及びその情報処理システムに関し、詳しくは、プログラムを不正に書換えたICカードを排除することができるようなICカード及びその情報処理システムに関する。

〔従来の技術〕

ICカードは、各種の金融機関カードとか職員カードなどに使用され、銀行のキャッシュカードとか、各種の商品取引におけるクレジットカード、そして交通機関の切符等の購入カード等に使用されつつある。

従来のICカードは、RAMをデータメモリとして使用しているためにデータ保持のための電源が必要となり、カード自体を薄くできないことと、保持する記憶容量が制限され、しかもデータの信頼性が十分であるとは言えなかった。

このような欠点を解消するために最近ではICカード側に電源を不要とした電氣的に消去可能なEEPROMをメモリとして使用するものが考えられている。

一方、ICカードの利用範囲は広く、銀行をはじめ、各種の商品取引に応じて発行されるICカードは、それぞれに応じて処理すべきデータの内容、処理の仕方が相違している。このようなことから、ICカードの処理プログラムは、それが使用される端末に対応したものとなっている。

そこで、銀行対応とか、各種の商品取引対応の端末装置に対応してICカード側にそれぞれ対応する処理プログラムを後から書込む、いわゆるダウンロード処理のICカードが提案され、例えば特開昭61-211788号等により公知となっている。

〔解決しようとする問題点〕

このようなダウンロード方式のICカードにあつては、その後の処理プログラムの改良、変更が比較的容易であり、ICカード自体の処理に柔軟性を持たせられるという大きな利点はあるが、ICカードが各種の商品取引に使用され、現金受け渡しの代わりとされ、ダウンロードによりICカード側に書込み可能な状態で処理プログラムを置くことから、その処理プログラムが改造されて悪用される危険性が高い。

この発明は、このような問題点を解決するものであつて、ICカードにおける処理プログラムが書換えられたか否かがチェックできるようなICカード及びそのICカード情報処理システムを提

供することを目的とする。

〔問題点を解決するための手段〕

このような目的を達成するための第1の発明のICカードは、演算処理装置とこの演算処理装置が実行する第1の処理プログラム、そのデータ及び更新情報を記憶する消去可能な第1の記憶手段と前記演算処理装置が実行する消去不可能な第2の処理プログラムを記憶する第2の記憶手段とを備えていて、第1の処理プログラムは挿着される情報処理装置側から書込まれるものであり、更新情報は第1の処理プログラムの全部又は一部が書換えられたときに書換えられた回数を示し、第2の処理プログラムは情報処理装置からの制御信号に応じて第1の処理プログラムの全部若しくは一部の書込み、更新情報の読出し及び第1の処理プログラムの全部若しくは一部の書込みに応じて更新情報の値を加算若しくは減算する処理を行うである。

さらに、第2の発明は、第1の発明におけるICカードが挿着されたときこのICカードとデー

タの授受を行いつつ第1の処理プログラムと更新情報とを有してICカードにこれらを書込む制御をする情報処理装置とを含めたICカード情報処理システムにある。

〔作用〕

このように処理プログラムの書換え等に対応して自動更新される更新情報をICカード側の電氣的に消去可能な記憶手段に記憶しておき、かつこの更新情報を読出せるようにしておけば、このICカードが挿着されるホストコンピュータ側で更新情報を読出して、ホストコンピュータ側の更新情報と比較することにより、処理プログラムがホストコンピュータ以外で書換えられたか否かを検出でき、不正な書換えを行ったICカードをチェックできる。

〔実施例〕

以下、この発明の一実施例について図面を用いて詳細に説明する。

第1図は、この発明のICカード情報処理システムを適用した一実施例のブロック図、第2図は、

そのプログラム更新情報比較処理のフローチャートである。

1は、ICカードであり、リーダ・ライタを有するホストコンピュータ(端末を含む。この明細書において同じ)2に挿着されて使用される。ICカード1は、その内部にマイクロプロセッサ11、マイクロプロセッサ11の制御プログラムを記憶したマスクROM12、処理プログラムのバージョンと書換え回数等を示す更新情報を記憶するEEPROM13、各種のアプリケーション処理プログラムを記憶するEEPROM14、ホストコンピュータ2との間で授受されるデータを記憶するEEPROM15、そして入出力インタフェース16とで構成されている。

マイクロプロセッサ11は、インタフェース16を介してホストコンピュータ2に制御されて、データ交換を行い、EEPROM13とEEPROM14、EEPROM15とは、それぞれマイクロプロセッサ11のアドレス空間に配置されて、そのバス17を介してアクセスされる。

ここで、EEPROM13に記憶される更新情報は、2つのものから構成され、その1つは更新回数を示す書換え回数情報13aであり、他の1つは、第1のプログラムの更新に応じて情報処理装置から書込まれる処理プログラムについてのバージョン情報13bである。書換え回数情報13aは、マスクROM12に格納されたカウント処理プログラム12aによりEEPROM14の処理プログラムが書換えられる都度、その値が1ずつ加算されてカウントアップされる。

なお、マスクROM12には、上記カウント処理プログラム12aの他に、処理プログラムの書込み、消去、書換え及び書換え回数情報13aとバージョン情報13bとの2つの更新情報の読出しを行う更新情報読出し処理プログラム12b、そのほかの各種の処理プログラムが格納されている。また、上記2つの更新情報を記憶するEEPROM13は、ここでは独立に設けているが、これは、このような更新情報のみならず、処理プログラムの種別を表す名称その他の情報を格納する

領域でもある。

ここで、EEPROM14に書込まれる処理プログラムの例としては、EEPROM15のデータの書込み、読出し、ホストコンピュータ2側から入力されるパスワードの照合等の処理プログラムであり、その最後のエリアには処理プログラムのスタートアドレス等が格納されていて、このアドレスがマスクROM12のプログラム等でアクセスされることになる。

一方、ホストコンピュータ2には、前記EEPROM14に記憶される処理プログラムとこの処理プログラムについてのプログラムのバージョン情報と書換え回数情報との2つからなる更新情報がメモリ3に記憶されていて、ダウンロードによりマイクロプログラム11を介して処理プログラムのバージョン情報と処理プログラムとをICカード1に書込む。したがって、EEPROM13のバージョン情報13bは、通常は、ホストコンピュータ2のものと一致する。

なお、この場合、書換え回数情報はICカード

1側に送出されず、処理プログラム書込みのごとに独立にホストコンピュータ2側でその値が1ずつ加算してされて更新される。一方、ICカード1側でも書換え回数情報13bがホストコンピュータ2からの書換え処理に応じて1ずつ加算してされて更新される。

このようなホストコンピュータ2のプログラムのバージョン情報と書換え回数情報とからなる更新情報と、ICカード1に格納された処理プログラムの書換え回数情報13aとバージョン情報13bとからなる更新情報とを区別するために、ホストコンピュータ2の更新情報が後に比較対象となるので、ここでは、ホストコンピュータ11の保有するホストコンピュータ側の更新情報（通常は、ICカード1側の書換え回数情報13a及びバージョン情報13bと同じものである）を比較情報Cとし、それがメモリ3に記憶されているものとする。さらに、メモリ3には、各種の制御プログラムの他に更新情報を比較する更新情報比較処理プログラム4が格納されている。

ところで、比較情報Cは、EEPROM14に記憶された処理プログラムの種別に応じて複数設けられているが、ここでは、例えばICカード1が特定の銀行におけるキャッシュカードのように特定のICカードであり、EEPROM14には、この特定のICカード1に対応する処理をするような処理プログラムが記憶されているとし、それに対する更新情報として説明する。

さて、ホストコンピュータ2は、ICカード1が挿入されたとき、それに電源を供給する。マイクロプロセッサ11と各EEPROM13とEEPROM14、EEPROM15とは、これにより電力の供給を受けて動作し、マイクロプロセッサ11のリセットが解除された時点で、マスクROM12のプログラムが起動されて、ホストコンピュータ11からの指令信号を待つ状態に入る。

ここで、ホストコンピュータ2は、第2図の処理に従ってまず更新情報比較処理プログラム4を起動して次の処理を実行する。すなわち、そのステップ①にて、プログラム更新情報読出し制御信

号をICカード1に対して送出して、ステップ②で更新情報入力待ちループに入る。

ICカード1がプログラム更新情報読出し制御信号を受けると、マスクROM12上の更新情報読出し処理プログラム12bを起動して、EEPROM13の書換え回数情報13aとバージョン情報13bとを読出し、これらをインタフェース16を介してホストコンピュータ2へと送出する。

ホストコンピュータ2が、これら書換え回数情報13aとバージョン情報13bとを受けると、ステップ③へと移り、ステップ④にて、ICカード1の処理プログラムに対応して保持してある比較情報C（ホストコンピュータ側の書換え回数情報とバージョン情報）をメモリ3から読出してこれらをそれぞれ比較する。その結果、これらそれぞれについて一致しているときには、ステップ④にて、処理プログラムを起動する制御信号を発生してICカード1に送出する。ICカード1は、この制御信号を受けて、マスクROM12に記憶された制御プログラムに従ってEEPROM14

に記憶された処理プログラムを起動し、それを実行する。

一方、ホストコンピュータ2は、次のステップ④において、商品取引の際の代金の清算とか、銀行における現金の引出し等に対して行われる通常のデータ処理とデータの授受を、挿入されているICカード1に対して開始する。ICカード1は、ホストコンピュータ2とデータの授受をEEPROM14に記憶された処理プログラムに従って行う。その結果、EEPROM15には、その取引等に応じた残高等の新しいデータが順次記憶されて行くことになる。

このような処理が終了すると次のステップ⑤にて、プログラム更新処理をすべきか否かを判定して、あらかじめ更新処理が指定されているときには、ステップ⑥にてICカード1に対してプログラムの書換え制御信号を発生して新しい処理プログラムとバージョン情報13bの書換えを行う。このときのバージョン情報は、書換えた処理プログラムについてのものであり、前のバージョン情

報13bとは相違している。それが数値であれば、数値が増加若しくは減少する状態に更新され、そうでなければ以前と相違する記号とされる。

ここで、ICカード1が書換え制御信号を受けると、ICカード1は、カウント処理プログラム12aを起動して、マスクROM13aの書換え回数情報13aを1だけカウントアップする。次にICカード1は、マスクROM12の書換え制御プログラムを起動して、EEPROM13のバージョン情報13bをホストコンピュータ2から送られた新しいバージョン情報に書換え、ホストコンピュータ11から送られて来る情報をEEPROM14に書込んで行く。

その結果、ICカード1のEEPROM13の処理プログラムのバージョン等が更新されるとともに、EEPROM14のアプリケーション処理プログラムが更新される。このとき、ホストコンピュータ2側においては、ステップ⑦において、書換え回数情報を1つ加算してバージョン情報を更新し、メモリ3の比較情報Cを更新したEEP

ROM13のものと一致するように書換える。

ここで、ステップ⑤の更新処理の指示は、ホストコンピュータ2に設けられたキーボード等からオペレータによりあらかじめ入力されて指示される。このような更新処理の指示がなければ、ステップ⑤の判定の後に処理はそのまま終了する。また、ステップ⑥で書換え回数情報13aとバージョン情報13bと比較した場合にいずれか一方が一致していなければ、ステップ⑥aにおいて、ICカード1とのデータ授受処理が中止されて、ディスプレイ等のその旨のメッセージ等が表示される。そして、ステップ⑦にて個別的なICカードの正当性のチェックを行い、正当なものについては、ここで現在の書換え回数情報13aとバージョン情報13bに書換えることができる。

なお、以上は、書換え回数情報13aとバージョン情報13bとの2つについて一致を検出した後に、ICカード1とのデータ交換を行い、これが終了した時点で処理プログラムを更新しているが、これらの一致を検出した後に、先に処理プログラ

ムを更新し、それからICカード1とデータ交換を行ってもよい。

ここで、書換え回数情報は、ホストコンピュータ2側とICカード1側とで独立に処理プログラムの書換えのごとに更新されるので、万一ICカード1側で他の情報処理装置により書換えられて、改造されて悪用されるようなことがあると、ICカード1側のカウント情報が1つ進み、ホストコンピュータ2側の書換え回数情報がそのままとなる。その結果、これらが一致しないことになり、それを検出することが可能となる。

ところで、前記ステップ⑤のプログラム更新処理をすべきか否かを判定に対して、プログラム更新処理の指示を定期的に行い、その都度バージョン情報13bを変更して行くようにすれば、ICカードにおける処理プログラムの状態を最新のものとすることができる。そこで、バージョン情報の一致をチェックすることにより最新ICカードに対してデータの授受を行うことができ、不正なICカードを排除できる。なお、最新の処理プロ

特開昭63-298588(6)

グラムに対応するバージョン情報13bを保有していないICカードについては、ステップ⑦で示したように個別に処理して正当なものであれば、最新の処理プログラムのバージョン情報に書換えることにより、継続的に使用可能である。

具体的な処理プログラムの書換え及びバージョン情報13bの更新周期又はバージョン情報だけの更新周期(単にバージョン情報のみを書換える場合)は、例えば1箇月ごととか、不正使用の可能性が生じたとき及びプログラムを変更したときとかに設定することができる。なお、後者の場合には、ほとんどICカードの自動書換えが済む期間として1箇月程度の余裕置いてから行い、ステップ⑧のバージョン情報13bの一致判定で一致しないものを排除するようにするとよい。

その結果、例えば、一年間以上の使用期間が空いたようなICカード等についての使用が排除され、現在使用されている有効な状態のICカードのみが継続的に使用できるようになり、ICカードの不正使用の可能性をさらに低減できる。

以上、この実施例では、更新情報として書換え回数情報とバージョン情報との2つを用いているが、これは、書換え回数情報だけでもよいことはもちろんである。さらに、ここでは、書込みをカウントするものであるが、ICカードの処理プログラムを読出すときに読出し回数をカウントする、読出し回数情報で同様なことを行うこともでき、不正をチェックすることができる。

また、書換えの検出をホストコンピュータからの書換え制御信号で行っているが、これは、書換えと処理プログラムの領域がアクセスされたことを持って行ってもよい。前記の読出しの場合の同様である。

実施例では、書換え回数情報を書込みが行われる都度、1ずつ加算しているが、これは減算であってもよく、その数は1に限定されない。

実施例では、更新情報を記憶するメモリを独立として更新情報のみならず、処理プログラムの種別を表す名称その他の情報を格納しているが、これは、処理プログラムを格納するEEPROMに

4の特定領域を割り当ててもよいことはもちろんである。したがって、処理プログラム、データ、そして更新情報とは同一の消去可能なメモリに記憶されていてもよく、また、それぞれ個別的な消去可能なメモリに記憶されていてもよい。したがって、実施例のように更新情報だけを取り出し、データ又は処理プログラムとを別個のメモリとしてもよい。このように個別にメモリデバイスに記憶される場合も含めてこのようなメモリをこの発明における第1の記憶手段としている。また、消去可能なメモリには、SRAMをはじめDRAM、フリップフロップのレジスタ、磁気メモリ等各種のメモリを挙げることができる。

[発明の効果]

以上の説明から理解できるように、この発明においては、処理プログラムの書換え等に対応して自動更新される更新情報をICカード側の電気的に消去可能な記憶手段に記憶しておき、かつこの更新情報を読出せるようにしておけば、このICカードが挿着されるホストコンピュータ側で更新

情報を読出して、ホストコンピュータ側の更新情報と比較することにより、処理プログラムがホストコンピュータ以外で書換えられたか否かを検出でき、不正な書換えを行ったICカードを検出できる。

4. 図面の簡単な説明

第1図は、この発明のICカード情報処理システムを適用した一実施例のブロック図、第2図は、そのプログラム更新情報比較処理のフローチャートである。

- 1…ICカード、2…ホストコンピュータ、
- 3…メモリ、11…マイクロプロセッサ、
- 12…マスクROM、13…更新情報を記憶するEEPROM、
- 13a…書換え回数情報、
- 13b…バージョン情報、
- 14…アプリケーション処理プログラムを記憶するEEPROM、
- 15…データを記憶するEEPROM、
- 16…入出力インタフェース、
- 17…バス。

第2図

第1図

